JOURNAL OF NUMBER THEORY **18**, 86–90 (1984)

On $Y^2 = X^3 + k$ and the Thue Rank of Cubic Curves

S. CHOWLA*

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

J. COWLES

Department of Computer Science, University of Wyoming, Laramie, Wyoming 82071

AND

M. COWLES*

University School, University of Wyoming, Laramie, Wyoming 82071

Communicated by H. Zassenhaus

Received February 22, 1982

The intersection of cords and tangents with the curve $Y^2 = X^3 + k$ is exploited to locate additional lattice points and to define the Thue rank of the curve.

A classical result due to Axel Thue shows that the number of lattice points (i.e., points with integral coordinates) on the curve $Y^2 = X^3 + k$ (k an integer) is finite. Let $N(k)$ be the number of symmetric pairs, $\langle X, \pm Y\rangle = \{(X, Y), (X, -Y)\}$, of lattice points on $Y^2 = X^3 + k$. The *tangent* to a pair $\langle X, \pm Y\rangle$ of points on the curve is a pair, $\langle \pm t\rangle = \{t, -t\}$, of lines with t tangent to the curve at (X, Y) and $-t$ tangent to the curve at $(X, -Y)$. The *cord* between the pair $\langle X_1, \pm Y_1\rangle$ on the curve and the pair $\langle X_2, \pm Y_2\rangle$ on the curve is a quadruple, $\langle \pm t_1, \pm t_2\rangle = \{t_1, -t_1, t_2, -t_2\}$, of lines with t_1 connecting (X_1, Y_1) and (X_2, Y_2), $-t_1$ connecting $(X_1, -Y_1)$ and $(X_2, -Y_2)$, t_2 connecting (X_1, Y_1) and $(X_2, -Y_2)$, and $-t_2$ connecting $(X_1, -Y_1)$ and (X_2, Y_2). A symmetric pair, $\langle X, \pm Y\rangle$, of points on the curve $Y^2 = X^3 + k$ is said to be on the tangent $\langle \pm t\rangle$ if and only if (X, Y) is on one of the lines t or $-t$ and $(X, -Y)$ is on the other. The pair $\langle X, \pm Y\rangle$ is on the cord $\langle \pm t_1, \pm t_2\rangle$ just in case for $i = 1$ or $i = 2$, (X, Y) is on one of t_i or $-t_i$ and $(X, -Y)$ is on the other. For a set S of pairs of points on the curve, let $S' = \{\langle X, +Y\rangle \mid \langle X, \pm Y\rangle$ is on a tangent to the curve at a pair in S or on a cord between two distinct pairs in $S\}$. For such a set S, let $S_0 = S$ and for $n > 0$, let

* The first and third authors acknowledge financial support from the Vaughn Foundation Fund.

0022-314X/84 $3.00

$S_{n+1} = S_n'$. Let $n_0 = \min\{n \mid S_n = S_{n+1}\}$. Then define the closure $\bar{S}$ of S to be S_{n_0}.

EXAMPLE. For the curve $Y^2 = X^3 + 17$, $N(17) = 8$, since the symmetric pairs $P_1 = \langle -2, \pm 3\rangle$, $P_2 = \langle -1, \pm 4\rangle$, $P_3 = \langle 2, \pm 5\rangle$, $P_4 = \langle 4, \pm 9\rangle$, $P_5 = \langle 8, \pm 23\rangle$, $P_6 = \langle 43, \pm 282\rangle$, $P_7 = \langle 52, \pm 375\rangle$, and $P_8 = \langle 5234, \pm 378661\rangle$ are all of the lattice points on the curve [2].

The tangent to $\langle -2, \pm 3\rangle$ is $\langle Y = 2X \pm 7\rangle$ and the pairs $\langle -2, \pm 3\rangle$ and $\langle 8, \pm 23\rangle$ are on this tangent. The cord between $\langle -2, \pm 3\rangle$ and $\langle -1, \pm 4\rangle$ is $\langle Y = \pm X \pm 5, Y = \mp 7X \mp 11\rangle$. The pairs $\langle -2, \pm 3\rangle$, $\langle -1, \pm 4\rangle$, $\langle 4, \pm 9\rangle$, and $\langle 52, \pm 375\rangle$ are on this cord.

Let $S = \{P_1, P_2, P_3\}$. Then, as the reader may verify, $S_0 = S$, $S_1 + S_0 \bigcup \{P_4, P_5, P_7\}$, and $S_2 = S_1 \bigcup \{P_6, P_8\}$. Thus, in this case, $\bar{S}$ contains all the pairs of lattice points on the curve.

Let the Thue rank, $T(k)$, of the curve $Y^2 = X^3 + k$ be defined to be the smallest integer n with the property that there is a set of S, of cardinality n, of symmetric pairs of lattice points on the curve, such that $\bar{S}$ contains all the pairs of lattice points on the curve. Thus, as an example, $T(17) = 3$.

The tables below are based on the tables found in [2]. The first table below records the values of k, $N(k)$, and $T(k)$ for those values of k between -100 and 100 for which $N(k)$ is exactly known and at least 2.

k	N	T	k	N	T	k	N	T
−76	2	2	15	2	2	63	2	2
−48	2	1	17	8	3	64	3	1
−11	2	2	24	4	3	65	4	2
−4	2	1	28	2	1	68	2	1
1	3	1	36	4	2	73	6	2
8	4	2	37	3	3	80	4	1
9	5	2	44	2	1	89	4	2
12	2	1	57	3	2	100	6	2

The next table provides information for those k between -100 and 100 for which $N(k)$ is not exactly known. $N'(k)$ provides a lower bound for $N(k)$ and $T'(k)$ is the Thue rank computed on the assumption that $N(k) = N'(k)$.

k	N'	T'	k	N'	T'
−100	3	1	−47	3	2
−63	2	1	−39	3	2
−60	2	1	−28	3	1
−55	2	1	−26	2	2
−53	2	2	−7	2	1

These tangents and cords can be used for locating lattice points on the curve $Y^2 = X^3 + k$. First formulae are needed for determining the intersections of the tangents and cords with the curve. The tangent $Y = mX + b$ to $Y^2 = X^3 + k$ at (X_1, Y_1) has slope $m = 3X_1^2/2Y_1$ and intercept $b = Y_1 - mX_1$. If the tangent meets the curve at (X_1, Y_1) and (X_2, Y_2), then X_1 and X_2 are zeros of $(mX + b)^2 = X^3 + k$ with X_1 being a double zero. Hence $2X_1 + X_2 = m^2$. Therefore for the tangent at (X_1, Y_1):

$$m = \frac{3X_1^2}{2Y_1}$$

$$X_2 = m^2 - 2X_1,$$

$$Y_2 = m(X_2 - X_1) + Y_1.$$

The cord $Y = mX + b$ to $Y^2 = X^3 + k$ between (X_1, Y_1) and (X_2, Y_2) has slope $m = (Y_2 - Y_1)/(X_2 - X_1)$. If (X_1, Y_1), (X_2, Y_2), and (X_3, Y_3) are where the cord intersects the curve, then X_1, X_2, and X_3 are the zeros of $(mX + b)^2 = X^3 + k$. Hence, $X_1 + X_2 + X_3 = m^2$. Therefore for the cord between (X_1, Y_1) and (X_2, Y_2):

$$m = \frac{Y_2 - Y_1}{X_2 - X_1},$$

$$X_3 = m^2 - X_1 - X_2,$$

$$Y_3 = m(X_3 - X_1) + Y_1.$$

EXAMPLE. From [3], it is known that $N'(255) = 13$. It is easy to discover that $P_1 = \langle -5, \pm 10 \rangle$, $P_2 = \langle 0, \pm 15 \rangle$, and $P_3 = \langle 10, \pm 35 \rangle$ are on the curve. The table below records the use of cords to discover an additional 10 pairs of lattice points on $Y^2 = X^3 + 225$.

	X_1	Y_1	X_2	Y_2	m	X_3	Y_3	
$P_1\ P_2$	−5	10	0	15	1	6	±21	P_4
$P_1\ P_2$	−5	−10	0	15	5	30	+165	P_5
$P_1\ P_3$	−5	−10	10	35	3	4	±17	P_6
$P_3\ P_5$	10	−35	30	165	10	60	±465	p_7
$P_1\ P_7$	−5	10	60	465	7	−6	±3	P_8
$P_2\ P_8$	0	−15	−6	3	−3	15	±60	P_9
$P_5\ P_9$	30	−165	15	60	−15	180	±2415	P_{10}
$P_3\ P_9$	10	−35	15	60	19	336	±6159	P_{11}
$P_4\ P_6$	6	−21	4	17	−19	351	±6576	P_{12}
$P_{11}P_{12}$	336	−6159	351	6576	849	720114	±611085363	P_{13}

Also from [3], $N'(1025) = 16$. Inspection shows that $P_1 = \langle -10, \pm 5 \rangle$, $P_2 = \langle -5, \pm 30 \rangle$, and $P_3 = \langle -1, \pm 32 \rangle$ are on the curve. The tangent at $(-10, 5)$ has slope $m = 30$, which shows that the pair $P_4 = \langle 920, \pm 27905 \rangle$ of points is also on $Y^2 = X^3 + 1025$. The remaining 12 pairs of lattice points on the curve can be found through the computation of cords.

	X_1	Y_1	X_2	Y_2	m	X_3	Y_3	
P_1P_2	−10	5	−5	30	5	40	±255	P_5
P_1P_2	−10	−5	−5	30	7	64	±513	P_6
P_1P_3	−10	5	−1	32	3	20	±95	P_7
P_3P_5	−1	−32	40	255	7	10	±45	P_8
P_1P_8	−10	5	10	45	2	4	±33	P_9
P_2P_8	−5	30	10	45	1	−4	±31	P_{10}
P_1P_{10}	−10	−5	−4	31	6	50	±355	P_{11}
P_8P_9	10	−45	4	33	−13	155	±1930	P_{12}
P_3P_9	−1	−32	4	33	13	166	±2139	P_{13}
P_3P_{10}	−1	−32	−4	31	−21	446	±9419	P_{14}
P_5P_{11}	40	−255	50	355	61	3631	±218796	P_{15}
P_2P_{10}	−5	−30	−4	31	61	3730	±277805	P_{16}

The following proposition is sometimes useful in the search for cords which intersect the curve at three lattice points.

PROPOSITION. *Let (X_1, Y_1) and (X_2, Y_2) be two lattice points on the curve $Y^2 = X^3 + k$. If $X_2 - X_1$ is a prime (or ± 1), then either the cord through (X_1, Y_1) and (X_2, Y_2) or the cord through (X_1, Y_1) and $(X_2, -Y_2)$ cuts the curve at a third lattice point.*

Proof. It is enough to show that the slope of the cord is an integer. Since $Y_1^2 = X_1^3 + k$, $Y_2^2 = X_2^3 + k$, and $Y_2^2 - Y_1^2 = X_2^3 - X_1^3 = (X_2 - X_1)(X_2^2 + X_2X_1 + X_1^2)$, it follows that either $(Y_2 - Y_1)/(X_2 - X_1)$ or $(Y_2 + Y_1)/(X_2 - X_1)$ is an integer.

Problems. Is there an integer n such that for all integers k, if $N(k) > n$, then $T(k) < N(k)$? The tables for $-100 \leqslant k \leqslant 100$ suggest $n = 3$ as a possibility, especially for positive k.

Is it the case that for all positive integers n, there is an integer k such that $N(k) = n$? The tables in [2] and [3] and the next proposition give some indication that the answer is yes.

PROPOSITION. *For all positive integers n, there is an integer k such that $N(k) \geqslant n$.*

Proof. A theorem of Lutz can be used to show that, for example, on the curve $Y^2 = X^3 + 17$ there are infinitely many points with both coordinates rational [4]. Choose n of these rational points on the curve: $P_1, P_2, \ldots, P_n$. For each P_i there are integers p_i, q_i, and r_i such that $P_i = (p_i/q_i^2, r_i/q_i^3)$ [1, p. 65]. Let M be the product of $q_1^6, q_2^6, \ldots, q_n^6$. Then k can be taken to be $17M$.

REFERENCES

1. S. CHOWLA, "The Riemann Hypothesis and Hilbert's Tenth Problem," Breach & Gordon, New York, 1965.
2. O. HEMMER, Notes on the diophantive equations $Y^2 - k = X^3$, *Ark. Mat.* **3** (1954), 67–77.
3. M. LAI, M. F. JONES, AND W. J. BLUNDON, Numerical solutions of the diophantive equation $Y^3 - X^2 = k$, *Math. Comp.* **20** (1966), 322–325.
4. E. LUTZ, Sur l'equation $Y^2 = X^3 - AX - B$ dans corps p-adiques, *J. Reine Angew. Math.* **177** (1937), 238–247.